## AMENDMENTS TO THE CLAIMS

Please amend claims 1 and 9 and add claims 17-19 as set forth below:

1.     (CURRENTLY AMENDED)     An authentication system used when stored information is manipulated, comprising:

a host computer comprising:

input means for inputting a user's instruction;

command output means for generating from the user's instruction an instruction command which requests a predetermined processing to be executed and for outputting the instruction command; and

communication means for communicating with an external unit; and

a fingerprint identification apparatus comprising:

communication means for communicating with said host computer;

processing control means for executing a predetermined processing according to the instruction command input from said host computer by said communication means;

fingerprint detection means for detecting a fingerprint and for generating fingerprint data;

storage-information recording means for recording the fingerprint data and storage information related to the fingerprint data; and

fingerprint identification means for verifying fingerprint data detected by said fingerprint detection means with the fingerprint data recorded by said storage-information recording means,

wherein said storage-information recording means stores a private key generated by the public-key encryption method, and

wherein said processing control means accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the user's instruction specifies a decryption of an encrypted text,

wherein said processing control means generates a symmetric key and a public key to encrypt the symmetric key when the user's instruction specifies an encryption of plain text, and

wherein ~~the user's instruction is one of a decryption of an encrypted text and an encryption of plain text, and~~ the user's instruction is sent to the host computer through communication cable.

2.    (PREVIOUSLY PRESENTED)    The authentication system according to Claim 1, wherein said storage-information recording means allows recorded storage information to be accessed only once immediately after the fingerprint-identification result is affirmative.

3.    (CANCELED).

4.    (PREVIOUSLY PRESENTED)    The authentication system according to Claim 1, wherein said fingerprint identification apparatus further comprises encryption processing means for generating an encryption key, for performing encryption by the use of the encryption key, and for performing decryption.

5.    (PREVIOUSLY PRESENTED)    The authentication system according to Claim 4, wherein said encryption processing means generates a public key and a private key according to the public-key encryption method, and decrypts an encrypted text by the use of the private key, wherein the encrypted text is received from the host computer and decrypted plain text is sent to the host computer.

6. - 8.  (CANCELED).

9.    (CURRENTLY AMENDED)    An authentication method used when stored information is manipulated, comprising the steps of:

a host computer informing a user of a fingerprint-identification request according to a user's instruction and issuing a fingerprint-identification instruction command to a fingerprint identification apparatus;

3

the fingerprint identification apparatus reading a fingerprint after the user places a finger on the fingerprint identification apparatus, verifying the read fingerprint with a stored fingerprint, and sending a fingerprint-identification result to the host computer;

the host computer allowing the user to specify the next instruction when the result is affirmative, and issuing the instruction command corresponding to the next instruction; and

the fingerprint identification apparatus accessing storage information according to the instruction command and executing a predetermined processing,

wherein said storage-information recording means stores a private key generated by the public-key encryption method, and

wherein the fingerprint identification apparatus accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the instruction command specifies a decryption of an encrypted text,

wherein the fingerprint identification apparatus generates a symmetric key and a public key to encrypt the symmetric key when the instruction command is one that specifies an encryption of plain text, and

wherein ~~the user's instruction is one of a decryption of an encrypted text and an encryption of plain text, and~~ the ~~user's~~ instruction command is sent to the host computer through communication cable.


10.   (PREVIOUSLY PRESENTED)   The authentication method according to Claim 9, wherein, in the step of the fingerprint identification apparatus accessing the storage information according to the instruction command and executing a predetermined processing, the storage information is allowed to be accessed only once immediately after the fingerprint-identification result is affirmative.


11.   (PREVIOUSLY PRESENTED)   The authentication method according to Claim 9, wherein the storage information includes a private key generated by the public-key encryption method, and in the step of the fingerprint

identification apparatus accessing the storage information according to the instruction command and executing a predetermined processing, a predetermined encrypted text is decrypted by the use of the private key, wherein the encrypted text is received from the host computer and decrypted plain text is sent to the host computer.

12. - 16.     (CANCELED).

17.     (REINSTATED-FORMERLY CLAIM 6)   A fingerprint identification apparatus in an authentication system used when stored information is manipulated, comprising:

communication means for communicating with a host computer;

processing control means for executing a predetermined processing according to an instruction command input from the host computer by said communication means;

fingerprint detection means for detecting a fingerprint and for generating fingerprint data;

storage-information recording means for recording the fingerprint data and storage information related to the fingerprint data; and

fingerprint identification means for verifying fingerprint data detected by said fingerprint detection means with the fingerprint data recorded by said storage-information recording means.

18.     (REINSTATED-FORMERLY CLAIM 7)   A fingerprint identification apparatus according to Claim 17, wherein said storage-information recording means allows recorded storage information to be accessed only once immediately after the fingerprint-identification result is affirmative.

19.     (REINSTATED-FORMERLY CLAIM 8)   A fingerprint identification apparatus according to Claim 17, wherein said fingerprint identification apparatus further comprises encryption processing means for generating an encryption key, for

C1 performing encryption by the use of the encryption key, and for performing decryption.